EXHIBIT A

ELECTRONIC FRONTIER FOUNDATION

November 30th, 2007

EFF Obtains Documents Detailing High-Level Battles Over Surveillance Law

Records Posted on EFF's Website

San Francisco - Today the Electronic Frontier Foundation (EFF) received the first of two batches of records from the Office of the Director of National Intelligence (ODNI) concerning the Administration's attempts this past summer to enact the Protect America Act and eviscerate the Foreign Intelligence Surveillance Act (FISA).

The records reveal new details about the contentious negotiations between Director of National Intelligence Mike McConnell and members of Congress that resulted in the passage of the Protect America Act -- an expansion of spying powers that undermined the Constitution and the privacy of Americans. In one letter, Senate Select Committee on Intelligence Chairman John D. Rockefeller IV claims that McConnell made "assurances" and "agreements" that were not carried out, and says, "I and others involved in these important and intense FISA negotiations are left to question whether the negotiations were carried out in good faith or whether your commitments were overruled by others at the White House or within the Administration." Senator Sheldon Whitehouse also expressed "deeply felt displeasure with the administration's legislative strategy on the recent 'FISA Fix'" and says that the Protect America Act was passed "at a substantial price, one that will be paid in rancor, suspicion and distrust."

"These documents give Americans a unique inside look at high-level discussions about how a controversial -- and critically important -- change to the law occurred," said EFF Staff Attorney Marcia Hofmann. "A Senate vote on more changes to FISA is just weeks away, and these records could not be more relevant to the ongoing debate on these issues."

EFF sued for the release of the records under the Freedom of Information Act (FOIA) earlier this year, demanding documents concerning briefings, discussions, or other contacts ODNI officials have had with representatives of telecommunications companies or members of Congress about amending FISA. Today's 250-page disclosure focuses on communications between ODNI and members of Congress but includes no information about the telecom industry's lobbying efforts. A federal judge ordered ODNI to release the rest of the relevant documents by December 10.

EFF represents the plaintiffs in Hepting v. AT&T, a class-action lawsuit brought by AT&T customers accusing the telecommunications company of violating their rights by illegally assisting the National Security Agency in domestic surveillance. The Hepting case is just one of many suits aimed at holding telecoms responsible for knowingly violating federal privacy laws.

Part one of the ODNI documents:
http://www.eff.org/files/filenode/foia_C0705278/113007_odni01.pdf

Part two of the ODNI documents:
http://www.eff.org/files/filenode/foia_C0705278/113007_odni02.pdf

For more on EFF v. ODNI:
http://www.eff.org/issues/foia/cases/C-07-05278

Contacts:

Marcia Hofmann
Staff Attorney
Electronic Frontier Foundation
marcia@eff.org

Kurt Opsahl
Senior Staff Attorney
Electronic Frontier Foundation
kurt@eff.org

David Sobel
Senior Counsel
Electronic Frontier Foundation
sobel@eff.org

Related Issues: *FOIA Litigation for Accountable Government (FLAG) Project*

Related Cases: *FOIA: Telecom Lobbying Records*

[Permalink <http://www.eff.org/press/archives/2007/11/30>]

EXHIBIT B

ELECTRONIC FRONTIER FOUNDATION

December 11th, 2007

EFF Obtains Government Documents on Congressional Intelligence Briefings

Records Released As Lawmakers Debate Changes to Surveillance Law

San Francisco - The Electronic Frontier Foundation (EFF) has received a second set of records from the Office of the Director of National Intelligence (ODNI) detailing behind-the-scenes briefings for lawmakers working to make substantial changes to the Foreign Intelligence Surveillance Act (FISA).

EFF requested release of the records under the Freedom of Information Act (FOIA) earlier this year, but ODNI dragged its feet in response. Last month, a federal judge ordered ODNI to release all documents by December 10. The first batch of records, made public on November 30, detailed contentious negotiations between Director of National Intelligence Mike McConnell and members of Congress that resulted in the passage of the Protect America Act -- an expansion of spying powers that undermined the Constitution and the privacy of Americans.

The second set of records contains more correspondence between McConnell and members of Congress, as well as heavily redacted versions of classified testimony delivered to the Senate Select Committee on Intelligence, and an FAQ detailing how the National Security Agency performs electronic surveillance. Withheld records include ODNI presentation slides used to brief Congress on foreign intelligence issues, and other classified documents.

"Our democratic system works best when citizens are fully informed about the issues being debated in Congress," said EFF Staff Attorney Marcia Hofmann. "Unfortunately, the Bush Administration is continuing to withhold information that is central to the pending debate on proposed changes to surveillance law."

The Protect America Act expires in February, and lawmakers are working on an extension of the bill -- potentially including more power for the government to spy on Americans as well as possibly granting amnesty for telecommunications companies that participated in the warrantless surveillance. EFF's Freedom of Information Act request also asked for any documentation of lobbying activity from telecoms that are facing lawsuits because of their role in the illegal spying. However, according to ODNI, the agency located a single document on this subject -- classified handwritten notes made by an ODNI employee on a telephone message slip.

EFF represents the plaintiffs in Hepting v. AT&T, a class-action lawsuit brought by AT&T customers accusing the telecommunications company of violating their rights by illegally assisting the National Security Agency in domestic surveillance. The Hepting case is just one of many suits aimed at holding telecoms responsible for knowingly violating federal privacy laws.

Part one of the ODNI documents:
http://www.eff.org/files/filenode/foia_C0705278/121007_odni01.pdf

Part two of the ODNI documents:
http://www.eff.org/files/filenode//121007_odni02.pdf

ODNI declaration explaining withholdings:
http://www.eff.org/files/filenode/foia_C0705278/121007_hackett_decl.pdf

For more on EFF v. ODNI:
http://www.eff.org/issues/foia/cases/C-07-05278

Contacts:

Marcia Hofmann
Staff Attorney
Electronic Frontier Foundation
marcia@eff.org

David Sobel
Senior Counsel
Electronic Frontier Foundation
sobel@eff.org

Related Issues: *NSA Spying*

Related Cases: *FOIA: Telecom Lobbying Records*

[Permalink <http://www.eff.org/press/archives/2007/12/11>]

EXHIBIT C

SFGate.com

AT&T case lobbying yields just one document, federal spy chief says

Bob Egelko, Chronicle Staff Writer
Wednesday, December 12, 2007

The Bush administration's top intelligence official, responding to a court order, reported Tuesday that his office had located only one document showing lobbying contacts with telecommunications companies about a pending surveillance bill - notes of a phone conversation that were too sensitive to release.

The records were sought by the Electronic Frontier Foundation, which represents customers in a lawsuit filed against AT&T in federal court in San Francisco. The suit accuses the company of illegally giving a federal agency access to phone calls, e-mails and customer databases for the government's program of monitoring communications between Americans and suspected foreign terrorists.

President Bush, who ordered the surveillance six years ago without congressional or court approval, has demanded that Congress protect telecommunications companies from lawsuits for their alleged collaboration with the program. He says companies should not be exposed to potentially ruinous damage awards for cooperating in an effort to enhance national security.

Lawmakers are scheduled to vote this month on Bush's proposal, which would scuttle the AT&T lawsuit and dozens of others pending before U.S. District Judge Vaughn Walker in San Francisco.

Arguing that the public should learn about company lobbying before the vote, the Electronic Frontier Foundation filed a Freedom of Information Act request Aug. 31, seeking records of contacts between the office of National Intelligence Director Michael McConnell, telecommunications companies and members of Congress.

When McConnell's office said it couldn't review the records before the end of the year, U.S. District Judge Susan Illston ordered a response by Dec. 10.

On Tuesday, the office produced hundreds of pages of documents on exchanges with Congress, some of them blacked out, but said it had found just one record of a contact with a telecommunications company.

"This document is a telephone message slip that contains the handwritten personal notes and mental impressions of an (office) employee," John Hackett, information management director for McConnell's office, said in a legal filing.

He said the document was being withheld because it is not an official record and because it is legally exempt from disclosure for a variety of reasons, including the need to protect classified information and personal privacy.

Marcia Hofmann, a lawyer with the Electronic Frontier Foundation, said the government will have to give Illston a fuller description of the document and the reasons for nondisclosure, probably after the congressional vote.

"We certainly had hoped to see more and we're surprised that they didn't locate more," Hofmann said. "It certainly raises questions about whether the search was comprehensive enough."

E-mail Bob Egelko at begelko@sfchronicle.com.

http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/12/12/MN1FTSBTV.DTL

This article appeared on page **A - 11** of the San Francisco Chronicle

EXHIBIT D

December 11, 2007 3:31 PM PST

Declassified docs show fight over surveillance, telecom immunity

Posted by Declan McCullagh | 1 comment

The Bush administration has released formerly classified documents that show how it is pressing Congress to rewrite surveillance law and immunize telecommunications companies from lawsuits.

What's also interesting about the documents, which were released in response to the Freedom of Information Act on Monday, is how much is redacted. Entire pages have been excised, in one case leaving only two paragraphs visible.

A few highlights from the the files (1 and 2) obtained by the Electronic Frontier Foundation after a court battle:

• **Pages 6-8 of file 1:** National Intelligence Director Mike McConnell told Congress three months ago that surveillance red tape required intelligence agencies to wait 12 hours to tap an Iraqi phone number--a claim that already has been called into question.

These documents give a detailed timeline that doesn't exactly jibe with what McConnell claimed. They say that the the NSA notified the Justice Department at 12:53 p.m. on May 15 that it believed it had the authorization to conduct domestic eavesdropping in this situation. The Justice Department received a formal request at 5:15 p.m. Because Attorney General Alberto Gonzales was traveling, he was not able to authorize it until 7:18 p.m. That's not exactly 12 hours.

• **Page 35 of file 1:** McConnell argues in a "TOP SECRET" document that retroactive immunity for AT&T and other telecommunications companies is necessary: "It is equally critical that private entities that are alleged to have assisted the (intelligence community) in preventing further attacks on the United States be insulated from liability for doing so."

So that's all the nation's top spook is willing to say in a "TOP SECRET" document? Maybe "TOP SECRET" classifications are like U.S. dollars: They used to be worth a lot more than they are today.

• **Pages 59-64 of file 1:** In a kind of governmental FAQ, the National Security Agency claims that its "minimization procedures" that limit electronic eavesdropping of U.S. citizens protect Americans' privacy rights. If the NSA is targeting a foreigner overseas, it says, its eavesdroppers will take extra precautions.

The NSA says, however, that it is "not reasonable to impose time limits" on when it should "drop that individual"--a U.S. citizen inside the United States--as a person of interest. It also objects to enshrining those internal procedures in law, claiming it would "be difficult to change" if necessary.

• **Page 6 of file 2:** The Office of the Director of National Intelligence has located a "telephone message slip that contains the handwritten personal notes" from an employee. It's being withheld under FOIA on four separate grounds--including that it's been classified.

TOPICS: Privacy
TAGS: NSA, wiretapping
BOOKMARK: Digg Del.icio.us Reddit

About The Iconoclast

Declan McCullagh has covered politics, technology, and Washington, D.C. for over a decade, which has turned him into an iconoclast and a skeptic of anyone who says: "We oughta have a new federal law against this."

Subscribe to this blog
Click this link to view this blog as XML.

Add this feed to your online news reader

The Iconoclast topics

Antitrust
Censorship
Corruption
intellectual property
Lessons in economics
Privacy
Regulation
Stupidity
Taxes

Latest blog posts from News.com

Gartner: Windows is collapsing
Posted in Beyond Binary by Ina Fried
April 10, 2008 8:31 PM PDT

Malcolm Gladwell tells security folks: Don't think too much
Posted in News Blog by Elinor Mills
April 10, 2008 6:39 PM PDT

Adobe releases debugged Lightroom 1.4.1
Posted in Underexposed by Stephen Shankland
April 10, 2008 5:18 PM PDT

Avoiding the Big One. It's not all that hard
Posted in Coop's Corner by Charles Cooper
April 10, 2008 4:52 PM PDT

Attention Flickr video haters: Try a free doughnut
Posted in Underexposed by Stephen Shankland
April 10, 2008 4:49 PM PDT

Featured blogs

Recent posts from The Iconoclast

FBI nudges state 'fusion centers' into the shadows

Home automation system, YouTube nab burglars

Lovestruck MySpace teen not guilty of harassment, court says

Pittsburgh couple sues Google over Street View

RIAA: N.Y. judge's 'making available' ruling was no setback

TalkBack

1 comments
Post a comment

Not that we needed any more proof
The_Decider
Dec 11, 2007, 9:56 PM PST

Read more comments >

Beyond Binary by Ina Fried
A look at how technology is changing our lives and at the people behind all that life-changing stuff.

Coop's Corner by Charles Cooper
Charles Cooper weighs in on Silicon Valley hijinks, and he doesn't suffer fools gladly.

Defense in Depth by Robert Vamosi
Covering the latest in computer viruses and computer crime.

Geek Gestalt by Daniel Terdiman
At the tech culture nexus of video games, fire art, and virtual worlds.

Green Tech
Fresh green tech news and commentary.

One More Thing by Tom Krazit
Tom Krazit takes on the tech phenomenon that is Apple, and keeps a close watch on the chip industry.

Outside the Lines by Dan Farber
When business and technology meet, that's when things get interesting.

The Social by Caroline McCarthy
Exploring all facets of social media and tech culture.

Underexposed by Stephen Shankland
Coverage of digital photography, science, and open-source software.

More CNET blogs »

EXHIBIT E

THREAT LEVEL

PRIVACY, SECURITY, POLITICS AND CRIME ONLINE

Top Spy Pushed Congress For Wider Powers, Citing High Summer Threat Level, Docs Show

By Ryan Singel | November 30, 2007 | 5:16:23 PM | Categories: NSA, Sunshine And Secrecy

The Director of National Intelligence urged powerful members of Congress to rush through legislation this summer that gave the NSA wide powers to install phone and internet wiretaps inside the United States, according to government sunshine documents released Friday.

The 242 pages of documents include letters to DNI Michael McConnell from members of Congress that are dated after the August 5 passage of the Protect America Act. They question whether McConnell negotiated in good faith or followed political orders from the White House.

The documents are the first to be released to the Electronic Frontier Foundation after a federal court judge on Wednesday ordered their prompt release.

In September, the EFF filed an Freedom of Information Act request about contact between the nations' top spy and telecom companies that want immunity from privacy lawsuits, as well as McConnell's contact with Congress.

The 242-page document (.pdf) includes detailed and revealing exchanges between Congress and McConnell, including one bitter letter from Sen. Jay Rockefeller (D-West Virginia), who clearly felt McConnell sucker punched him in the final moments of the debate over closing the government's so-called "intelligence gap."

That gap ostensibly referred to the fact that if the government wants to install surveillance equipment inside America or force companies like AT&T or Google to help it spy on people outside the United States, it had to get a court order.

After 9/11, the Bush administration believed it had the legal right to avoid that requirement and launched a secret wiretapping program. A year after the program was revealed in December 2005, Bush bowed to political pressure and allowed the secret spying court to issue 'innovative orders' allowing the program to continue. But in the spring, another judge on that court decided the program was illegal. The administration then bum-rushed Congress for powers it could have asked for long ago, telling them Al Qaeda was coming and that blood would be on Congress's hands if they didn't immediately hand over

Qaeda was coming and that blood would be on Congress's hands if they didn't immediately hand over more powers to the administration.

These letters document McConnell's public and not-so-public role in the ongoing debate over reforms to the Foreign Intelligence Surveillance Act.

The rest of the responsive documents must be released by December 10, according to U.S. District Court Judge Susan Illston.

The documents are very detailed, and THREAT LEVEL has only had limited time to review them. Any help FISA-geek readers can give would be much appreciated. Drop nuggets from the doc (.pdf) (with page numbers) in the comments.

See Also:

- Top Spy Must Release Telecom Immunity Meeting Docs ASAP
- In Twist, Senate Judiciary Spying Bill Lacks Immunity for Telecoms
- Stage Set for Senate Immunity Showdown As House Passes Spy Bill ...
- Time Columnist Joe Klein Gets Wiretapping Debate Wrong a Third Time

danke

Posted by: bt | **Nov 30, 2007 5:48:14 PM**

Why does it seem like every time there's an important vote, it's time for a double-secret-orange-alert?

Posted by: | **Nov 30, 2007 5:51:25 PM**

Skimming the whole durn thing it doesn't look overwhelmingly juicy to me. It's helpful to get timelines straight, and there's interesting bits regarding the implementation of the Protect America Act since August. If you look at the file, there's a lot of redundant pages, fax transmission cover letters, and previously released witness statements from committee hearings - it seems that only the first six pages are particularly sensitive.

And on page 4 (of the PDF) there's hints that Ron Wyden is concerned about the rights of US citizens that work for US corporations that interact regularly with foreign corporations. This is kind of scary, and isn't this reminiscent of all the old claims that the ECHELON system was being used to commit economic espionage, claims given just a tad of credence by ex-DCI Woolsey's in his op-ed " Why We Spy on Our Allies" way back in 2000:
http://cryptome.org/echelon-cia2.htm

Are US-based employees of foreign corporations like BAE, EADS, SAP, Nortel, Vodafone, Samsung, NTT, Qinetiq, BP, Petrochina, Statoil, Lukoil, maybe even News Corp, all presently targeted without the need to get warrants? That warrants aren't even necessary when these employees speak with employees of US corporations? Is this "reverse targeting" of entire industry sectors?

Seems like this has nothing to do with the Global War On Terror and all about the administration spying on foreign corporations, not al-Qaeda calls from caves in Afghanistan. What was Wyden asking the DNI at this closed hearing on September 20? Intel's a big employer in Oregon - are there sensitive communications with Chinese suppliers being monitored now without the need for warrants?

And what's a "foreign corporation" anymore anyway, in this age of tax-dodging offshore shell companies, joint-ventures, and overseas affiliates? Is Accenture foreign? What about George Soros - if his foreign-registered mutual funds designate him as a foreign target, can his left-leaning NGOs be monitored

Zombie Computers Decried As Imminent National Threat

Feds Charge Porn Producer With Selling Adult Content to Adults

Industrial Control Systems Killed Once and Will Again, Experts Warn

Wiretapping Powers Debate Still Unsettled

Jury Can Consider Lesser 'Manslaughter' Verdict, Reiser Judge Rules

MOST RECENT ENTRIES

April 2008

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Government to Seek Terrorists in World of Warcraft: The Full Proposal

Feds Charge Porn Producer With Selling Adult Content to Adults

Wiretapping Powers Debate Still Unsettled

Industrial Control Systems Killed Once and Will Again, Experts Warn

Zombie Computers Decried As Imminent National Threat

U.S. Has Launched a Cyber Security 'Manhattan Project,' Homeland Security Chief Claims

Jury Can Consider Lesser 'Manslaughter' Verdict, Reiser Judge Rules

TIME Magazine Wins Threat Level's Competition for Best Blog-Rating Story

U.S. To Pitch 'Phase One' of Net Monitoring Plan at RSA

EU Tells Search Engines to Stop Creating Tracking Databases

without warrants? If Halliburton moves to Dubai will they be seen as foreign? I've got to review the document further to see if any follow-up has been included here regarding the monitoring of US corporations and minimization procedures. Though my guess is that's not declassified. Still interesting to ponder though.

Posted by: SPD | Nov 30, 2007 6:12:26 PM

Pages 44-47 seem to be germane, as they're part of a letter clarifying minimization procedures from the ODNI Civil Liberties Protection Officer to the House Intel committee chair and ranking member. Of course Reyes and Hoekstra haven't been the sharpest tools in the shed, so they might not've ever read this.

Posted by: SPD | Nov 30, 2007 6:23:06 PM

Oh yeah, and there's an illuminating distinction btwn the phases of surveillance. Acquisition is set apart from both monitoring and targeting, etc.

Posted by: SPD | Nov 30, 2007 6:25:28 PM

'nuff said. proud to have him represent my state.

Posted by: Ron Wyden Is Awesome | Nov 30, 2007 6:51:02 PM

The extreme deference that the DNI shows to a mere House member is striking on pages 56-7, but then Udall's family is pretty unique. Interestingly, he apparently has a solid position against retroactive immunity and seems to be concerned about the retention of "unintentionally" collected information. Udall taking a strong stance on this issue would indicate that, if he's the Democrat's choice for the open Senate seat in NM and Heather Wilson (ex-Air Force intelligence and surveillance oversight surrender-monkey) is the GOP's, then there's likely to be rhetorical fireworks on surveillance all the way through next November. Let's hope the media covers it in a grown-up way and highlights their different views. Portraying Wilson running for the legislative branch that she's sought to weaken is one example. But then again, maybe the US Attorney scandal will take her out of the picture.

Posted by: SPD | Nov 30, 2007 6:54:58 PM

FYI: page 240 is the judicial escape hatch for the current lawsuits. it allows transfer to FISC upon request by the AG.
"
Sec. 411 Mandatory Transfer for Review.
Section 411 would allow for the transfer of sensitive national security litigation to the Foreign Intelligence Surveillance Court... if: (1) the case is challenging the legality of a classified communications intelligence activity ... and (2) the Attorney General files an affidavit under oath that the case be transferred...
"

Posted by: DCS3000 | Nov 30, 2007 7:05:36 PM

On pages 71-3 , there should be no surprise that the spurned Harman led the Blue Dogs before the August recess in inviting the administration to throw out the meaning of the 4th Amendment. They insist on warrants for any Americans. But the Blue Dogs want to: "Authorize the FISA Court to issue a single order which approves your ability to conduct certain targeting operations in foreign countries."
Huh? As it's been often pointed out on TL, the NSA already had free reign abroad - why would the Protect America Act enhance their capabilities abroad, other than closing the technological 'loophole' re: communications routed through the US? But then what's this about "certain targeting operations" - why would these need a court order? Those actions are "in foreign countries" - and therefore totally beyond the scope of FISA...right?

There's two ways to see this, I guess. One: Are Americans' communications already "unintentionally" acquired in this targeting process done abroad? Oops. (Then what's the point of clarifying you need a warrant to target Americans if they can be swept up in basket targeting abroad? And then those intercepts can be kept if there's just "some" intelligence value?) Particularization of warrants for targeting Americans but not asking the NSA to check whether there's any Americans amongst those monitored en masse leaves a hole big enough to drive a multinational corporation through.

Two. Another way that "certain targeting operations" could make sense would be in the logistics and implementation of such a program, which is always kept fuzzy. How about purposely routing foreign-to-foreign traffic through the US, for no reason other than to make it easier to wiretap? Ie hosting facilities having peering arrangements in the US (taking the SWIFT case as an example), and US telcos aggressively seeking joint ventures with domestic carriers abroad. NSA collusion with corporations? Perish the thought!

Or maybe its just (!) monitoring every instance of Hotmail or Gmail in Iran, regardless of whether or not the person at the keyboard holds a US passport and is just visiting her grandma over the summer?

On a related note, on pages 90-91 there's interesting stuff on the kidnapped soldiers timeline and probable cause standards being met in whats described as this "novel and complicated" scenario. Still not sure what happened there...was it merely collecting emails stored in the US? That wouldn't seem to be either "novel" and would only be "complicated" if they were doing a massive trolling through everything for certain phrases, etc. Were US phone lines or US phone cards used by the insurgents? Or are call records for Iraqi (or Jordanian or Kuwaiti) mobile phone operators located here in the US? Were the insurgents using terminals in Internet cafes with VSAT uplinks serviced by US firms?

CATEGORIES

Announcements (12)
Apple, iPhone (2)
BitTorrent (12)
Breaches (25)
California Fires (6)
CCC (20)
Censorship (41)
Copyrights and Patents (58)
Cover-Ups (33)
Crime (77)
Crypto (10)
Cybarmageddon! (19)
Cybersecurity (3)
DefCon (6)
Disasters (1)
E-Voting (52)
Election '08 (291)
Forensics (2)
Gists (3)
Glitches and Bugs (32)
Hacks and Cracks (108)
Hans Reiser Trial (83)
Hot Planet (24)
Identification (46)
Information Sharing (5)
Intellectual Property (8)
ISP Privacy Survey (10)
Kickbacks (7)
Mobile Phone Unlocking (1)
Network Neutrality (7)
NSA (126)
Online Political Campaigns (18)
Patents (1)
Phreaky Phriday (2)
Politics (70)
Porn (11)
Privacy (108)
RFID (4)
RIAA Litigation (40)
RSA Conference (6)
Spam and Phishing (7)
Spooks Gone Wild (57)
Sunshine and Secrecy (81)
Surveillance (122)
Tech Companies in China (8)

Posted by: SPD | Nov 30, 2007 8:26:58 PM

Regarding the clear-and-present-danger feeling that caused Michael Chertoff's guts to tingle this summer, I was impressed to see that the Dems in the Senate Judiciary Committee actually broke out their calculators in an attempt to pin down the location of FISA warrant application bottleneck:

"The Administration's report to Congress states that 2,181 FISA applications were filed in 2006. If each application takes 200 man-hours, as you suggested in the El Paso Times interview, this would require at least 218 attorneys and anaysts working full-time for more than 436,000 hours on nothing but warrant applications. Do you continue to stand by your assertion to the El Paso Times that "it takes about 200 hours" to do the application for each phone number?" [Page 145, Judiciary Committee letter dated Sept. 11, 2007, signed by Conyers, Nadler, and Scott, to DNI Mike McConnell]

There was no response from McConnell included in the pdf. Perhaps he has not yet answered, or answered in closed session.

Also, the House Permanent Select Committee on Intelligence tried to take issue with DNI Mike McConnell's statements about German terror plots:

"... Senator Leiberman asked you whether the so-called Protect America Act, which President Bush signed into law on August 5, 2007, facilitated the detection of the German terrorist plot.
"You responded, 'Yes sir, it did.'
"This statement is at odds with information I have received. Specifically, I am told by senior American officials that US assistance to German intelligence was based on collection under FISA several months before its modification by Congress in August. Accordingly, the new law did not lead to the arrests of the three terrorist plotters, as you claimed." [Page 148, House Permanent Select Committee on Intelligence letter dated Sept. 11 2007, signed by Reyes, to DNI Mike McConnell]

Again, there was no response from McConnell included in the pdf. Perhaps he has not yet answered, or answered in closed session.

Posted by: Jack Lint | Nov 30, 2007 11:39:22 PM

Apparently all communications are routed to surveillance software for storage and subsequent selective retrieval, followed by analysis as desired; not, surveillance software selectively routes communications of interest to storage.
I think the problem is, they seize everything and then search; even a court warrant does not allow that; that might be the problem.
I think they could redesign the hardware and software so it might be legal if FISA authorized it; maybe not.

Posted by: taptap who's there? nsa :(| Dec 1, 2007 9:25:56 PM

The phone system doesn't have separate communication lines for emails, Internet searches, data transfers, wired calls and wireless calls; it's all one; and the USA is the largest hub in that international system.
The phone system is designed to route and reroute communications however it is necessary to complete a voice or data or other transfer.
While phone calls have timing constraints that limit their routing, the Internet was deliberately designed to operate without routing constraints to ensure that, regardless of timing, packets of information would reach their intended recipients; browsers are deliberately designed to time out so you don't wait forever.
So for Internet applications why would national boundaries make any difference? (Unless, like China, you deliberately design your servers not to allow information to pass.) What's international and what's domestic when the Internet is involved?

Posted by: ET phone home | Dec 1, 2007 9:45:22 PM

Moving backwards, yes I certainly agree with @ET that there is virtually no segregation between voice and data services once they've reached the backbone, if not before then. But I would suggest that the US is not only the vital hub, but that machinations of capital, be they private equity acquistions or telco consolidation, have led to a present circumstance where the US is not only the hub for many purely foreign-to-foreign transactions, but that there are active government policies to enhance the intercept capabilities of US telco corporations. Sweetheart merger approvals and fat covert contracts go a long way in guiding corporate strategy. In the long run, many transoceanic fiber-runs and satellite services around the globe have found themselves US partners and therefore entwined with the NSA's global intercept capability.

Back to @taptap, I do think that there's a shell game being played here in public. Follow our meaning while we shift the phrases fast enough to make your head spin. Are we talking acquisition? Or targeting? Or monitoring? Michael Hayden has been particularly adept at oscillating between these phrases, but no one has seemed to put a particularly technical meaning to any of them. It would seem that targeting is where they decide to deploy resources, monitoring follows in a dragnet fashion, and then content collection only seems to have happened when a human analyst listen to it. Unfortunately under FISA, the coin of the realm is acquisition. Well didn't they violate that in the very first step, when they installed backbone wiretaps that mirrored all signals to be parsed and forwarded on? Oops. Gotcha.

Back to @JL, I do agree that Conyer's committee has mostly acted honorably on this issue. But he's been constantly undermined by vindictive folk such as Harman who's encouraged by other powerful actors like Hoyer and Tauscher.
Regarding the whole analyst labor-hours issue, my only comment is that it's become awfully difficult to keep staff in place in the Intelligence Community for the last several years. So maybe we're merely hearing the flip side of endless outsourcing - the peons left to do the paperwork don't work too fast.
Anyone catch Hayden's bragging over the summer about how 70% of the CIA workforce was hired in the last 18 months? (I'm almost sure I got the number right.) He was trying to emphasize the youthful

The Courts (44)
The Ridiculous (4)
Threats (46)
ToorCon (8)
Virginia Tech shootings (32)
Watchlists (24)
Wikiwatch (3)
Yo Ho Ho (1)

enthusiasm, the spirit of change in the air in the Intelligence Community. I call bullsh**.
As regards the German plot, I think that it was entirely foiled by Army CID doing their job at force protection, and then liaising with their German counterparts. No mystery there. Similar operations have been disrupted several times in the Frankfurt area since 9/11. Of course it's likely those very same folks also hyped up a vague threat so much that the Macedonians picked up al-Masri on a lark. Oops.

In any event, I also feel that there's a lot left classified. But wasn't this whole FOIA about telco lobbying anyway? What gives? I want to see Bradford Berenson's name on call sheets. Know what I mean?

Posted by: SPD | Dec 2, 2007 12:40:16 AM

taptap says all content is collected, consistent with Mark Klein formerly of AT that's the point; everything is acquired, for contemporary and historical analysis; acquire all content, then analyze selected targets.

Posted by: Hayden's creation at NSA b4 CIA assignment | Dec 2, 2007 4:03:08 PM

Has WIRED editors ever heard of SPELL CHECK.
I am big fan of WIRED magazine, but the online reporting is a joke. Spelling errors and poor grammer.
Are these articles written in their sleep?
SPELL CHECK please

Posted by: MAX | Dec 3, 2007 5:40:08 PM

POST A COMMENT

Name:

Email Address: (Not Required, Not Published)

Comments:

Post

See more Threat Level

EXHIBIT F

April 10, 2008

ABOUT ODNI
ODNI Home
Who We Are
Vision and Mission
ODNI Organization
ISE
NCTC
NIC
NCIX
SSC
CSE/NIEMA
History of the ODNI
ODNI Seal
FAQ
PRESS ROOM
Press Releases
100 Day Plan
500 Day Plan
Announcements
Speeches
Interviews
Congressional Testimonies
Reports
Publications
CAREERS
USA.gov
IC Careers
OPM-USAJobs
IC CAE
CONTACT US
Contact Information

Office of the Director of National Intelligence Electronic Reading Room

Records Requested under FOIA

- **Electronic Frontier Foundation Interim Response, 11-30-07**
- **Electronic Frontier Foundation Final Response, 12-10-07**

Intelligence Reports

- Reports to Congress
  - February 2008: **Data Mining Report**
  - February 2007: **2006 Annual Report of the United States Intelligence Community**
  - April 2006: **Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces**
- Miscellaneous Reports
  - April 3, 2007: **2006 IC Survey Results**
  - May 1, 2006: **2005 IC Survey Results**

Policy Documents

- Intelligence Community Policy Guidance
  - June 25, 2007: **Intelligence Community Policy Guidance (ICPG) 601.01** Intelligence Community Civilian Joint Duty Program Implementing Instructions
- Intelligence Community Directives
  - March 6, 2008: **Intelligence Community Directive (ICD) 702** Technical Surveillance Countermeasures
  - November 28, 2007: **Intelligence Community Directive (ICD) 651** Performance Mgmt Sys for the IC Workforce
  - October 17, 2007: **Intelligence Community Directive (ICD) 206** Sourcing Requirements for Disseminated Analytic Products
  - September 13, 2007: **Intelligence Community Directive (ICD) 204** Roles and Responsibilities for the National Intelligence Priorities Framework
  - August 29, 2007: **Intelligence Community Directive (ICD) 180** Intelligence Community History Programs
  - July 16, 2007: **Intelligence Community Directive (ICD) 202** National Intelligence Board
  - July 6, 2007: **Intelligence Community Directive (ICD) 302** Document and Media Exploration
  - June 25, 2007: **Intelligence Community Directive (ICD) 203** Analytic Standards
  - May 23, 2007: **Intelligence Community Directive (ICD) 655** National Intelligence Awards Program

- January 8, 2007: **Intelligence Community Directive (ICD) 200** Management, Integration, and Oversight of Intelligence Community Analysis
- December 21, 2006: **Intelligence Community Directive (ICD) 900** Mission Management
- October 3, 2006: **Intelligence Community Directive (ICD) 300** Management, Integration, and Oversight of Intelligence Collection and Covert Action
- August 16, 2006: **Intelligence Community Directive (ICD) 602** Human Capital: Intelligence Community Critical Pay Positions
- August 15, 2006: **Intelligence Community Directive (ICD) 105** Acquisition
- July 11, 2006: **Intelligence Community Directive (ICD) 301** National Open Source Enterprise
- May 17, 2006: **Intelligence Community Directive (ICD) 104** Budgeting for Intelligence Programs
- May 16, 2006: **Intelligence Community Directive (ICD) 601** Human Capital - Joint Intelligence Community Duty Assignments
- May 1, 2006: **Intelligence Community Directive (ICD) 1**
- April 21, 2005: **Intelligence Community Directive (ICD) 2005-1** System of Intelligence Community Directives: Status of Director of Central Intelligence Directives: Delegation to the Principal Deputy Director of National Intelligence

- 2007 Intelligence Community Policy Memorandums
  - **2007-200-2:** ICPM 2007-200-2, Responsibility to Provide
  - **2007-500-8:** ICPM 2007-500-1, Unevaluated Domestic Threat Tearline Reports

- 2006 Intelligence Community Policy Memorandums
  - **2006-100-1:** The Intelligence Community Policy Process
  - **2006-200-2:** Role of The Office of the Director of National Intelligence Analytic Ombudsman
  - **2006-600-1:** National Intelligence Reserve Corps (5mb)
  - **2006-700-3:** Intelligence Community Modifications To Annex C (25mb)
  - **2006-700-4:** Intelligence Community Modifications to DCID 6/4. "Personnel Security Standards and Procedures for Governing Eligibility for Access to Sensitive Compartmented Information (SCI), Annex A Standard C . Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)" (3mb)
  - **2006-700-5:** Intelligence Community Modifications to DCID 6/4 "Personnel Security Standards and Procedures for Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," Annex F "Reciprocity of SCI Eligibility Determinations" (6mb)
  - **2006-700-6:** Intelligence Community Modifications to DCID 6/4: "Personnel Security Standards and Procedures for Governing Eligibility for Access to Sensitive Compartmented Information (SCI)" Pertaining to Expeditious Handling of Issue-Free Personnel Security Cases and Out-Of-Date Single Scope Background Investigations for Continued and Renewed SCI Access (2mb)
  - **2006-700-7:** Intelligence Community Modifications to DCID 6/9. "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)" (3.5 mb)
  - **2006-700-8:** Intelligence Community Modifications to DCID 6/1 Supplement. "Security Policy Manual For SCI Control Systems"
  - **2006-700-10:** Intelligence Community Update to Director of Central Intelligence Directive 6/11 "Controlled Access Program Oversight Committee"

- 2005 Intelligence Community Policy Memorandums
  - **2005-100-3:** Reporting of Intelligence Activities to Congress

- **2005-400-1:** Authorities, Roles, and Responsibilities of the Deputy Director of National Intelligence for Customer Outcomes
- **2005-700-1:** Intelligence Community Update to Director of Central Intelligence DCID 6/9. "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)"
  - **Part I -Portable Electronic Devices in Sensitive 3 Compartmented Information Facilities**
  - **Portable Electronic Device (PED) Mitigation**
- **2005-800-1:** Authorities, Roles, and Responsibilities of the Deputy Director of National Intelligence for Science and Technology